

# C17A - Seguridad Informática

## Componente básicos de la seguridad

### **Seguridad activa y pasiva**

La seguridad de la información consiste en todas las acciones que llevamos adelante para proteger la integridad, la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. Para poder proteger a nuestra computadora tenemos dos tipos de seguridad: seguridad activa y seguridad pasiva.

### **¿Qué es la seguridad activa?**

Los elementos denominados activos contienen información, pueden tener muchas formas: servidores, dispositivos móviles, bases de datos, entre otros. Esos activos contienen información que alguien quiere vulnerar, obtener, destruir, etcétera. Como su intención es acceder a una información, lo va a hacer a través de una vulnerabilidad —problema que tienen los sistemas que contienen información—. La amenaza aprovecha esa vulnerabilidad para

ingresar de forma indebida a la información y hacer lo que quería hacer. La seguridad activa protege y evita daños en los sistemas informáticos.

Buenas prácticas:

- Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.
- Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
- Encriptar los datos importantes: La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información solo pueda ser leído si se conoce la clave de cifrado.

## ¿Qué es la seguridad pasiva?

Es un conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos. Estas acciones se activan cuando se ha introducido un malware o cualquier otra amenaza en los sistemas.

Buenas prácticas:

- La realización de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas.
- Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
- Crear particiones en el disco duro para almacenar archivos y backups/copia de seguridad en una unidad distinta a donde tenemos nuestro sistema operativo.
- Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.

- Es importante que cuando haya una infección por un virus, comprobar que el antivirus funcione correctamente.

## Medidas de protección

### ¿Qué es el control?

Cuando hablamos de control solemos encontrar muchas definiciones, la RAE (Real Academia Española) lo define como comprobación, inspección, fiscalización e intervención. En otras fuentes, podemos encontrar que es el conjunto de los mecanismos, acciones y herramientas realizadas para detectar la presencia de errores. Sin embargo, en este curso nos vamos a referir a control como un proceso que consiste en una paridad entre un resultado con otro.

Muchas veces se piensa que la seguridad de la información consiste solo en implementar controles técnicos. Pero para que esta seguridad sea integral sobre los equipos y software informáticos se deben implementar también algunos controles de tipo administrativo y físicos. A continuación, veremos algunas de esas clases de controles.

# Clases de medidas de seguridad

## Proactivas



## Reactivas



### Directivas

Nos dicen qué podemos o no hacer. Intentan que las actividades de los sistemas se realicen de una manera específica con el fin de que se produzcan ciertos resultados esperados.

### **Disuasivas**

Pueden desviar la intención del atacante potencial a un sistema o el uso indebido por parte del personal. Se diferencian con las directivas en que estas no nos restringen directamente, sino que nos hacen una advertencia, la cual se puede o no tener en cuenta a la hora de ejecutar la acción indebida.

### **Preventivas**

Buscan que no se produzca un accidente o cualquier tipo de acción indebida en los sistemas. La diferencia con las disuasivas es que estas buscan informar y prevenir una acción indebida.

### **Detectivas**

Se basan en la búsqueda de potenciales ataques o peligros a los que puede estar expuesto un sistema informático.

## Correctivas

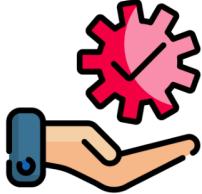
Una vez se ha encontrado el riesgo o ha sucedido un incidente que ha puesto en peligro a los datos o información, se activan estas medidas de seguridad. Su objetivo es solucionar el sistema luego que ha sucedido el desvío.

## Introducción a auditoría

Auditar es la acción de analizar de manera exhaustiva y profunda las distintas características y áreas de una organización. En informática, el auditor es el encargado de analizar y determinar que toda la informática de la organización trabaje de manera eficiente.



## Objetivos de la auditoría de sistemas de información



### EFICIENCIA

Se debe trabajar de manera tal que la información recabada sea útil para la toma de decisiones.



### NORMATIVA

Se deben cumplir las normativas determinadas para certificar que la empresa trabaja bajo las normas estándares.



### GESTIÓN DE RECURSOS

Recursos utilizados de manera correcta.

Auditoría

DigitalHouse >  
Coding School

## Conocimientos del auditor informático

Para cumplir con los objetivos mencionados anteriormente, es necesario:



### EFICIENCIA

Experiencia en gestión de proyectos.



### NORMATIVA

Conocimiento de softwares y normativas.



### GESTIÓN DE RECURSOS

Conocimiento de Infraestructura.

Auditoría

DigitalHouse >  
Coding School

## Auditor

La mayoría de los auditores trabajan en **pequeños grupos** de hasta 4 personas y son el nexo directo con los distintos departamentos y dirección.

El auditor informático **plasmará** en un **informe final** todas las debilidades, oportunidades de mejora y recomendaciones para que la organización **sin carácter obligatorio** decida si aceptarlas o no.



## Herramientas para auditar

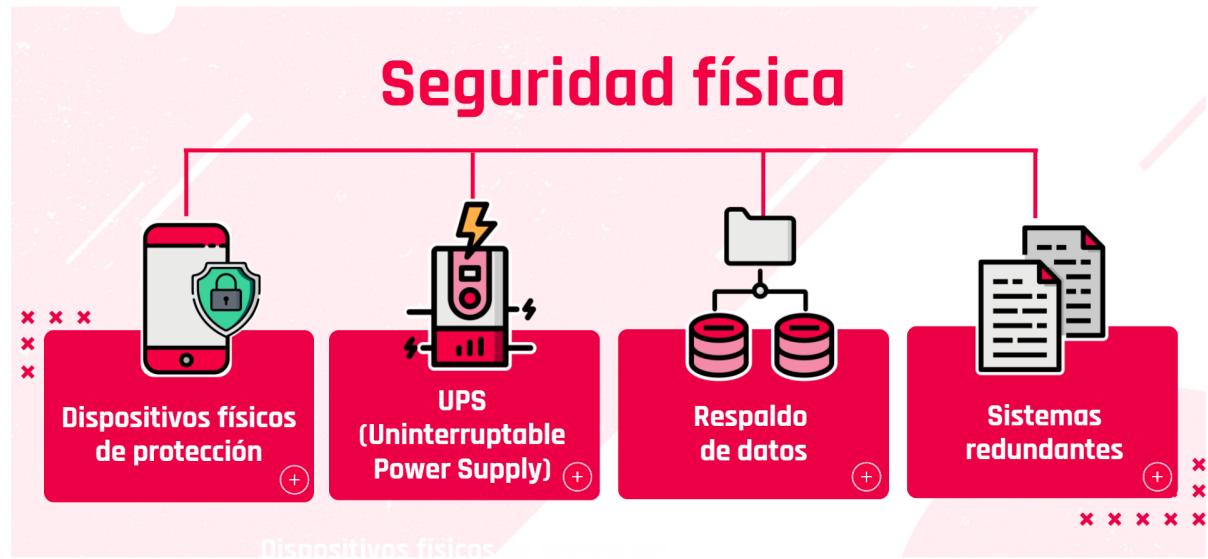
Estas son **algunas** de las herramientas más **comunes** que utiliza el auditor:

| Conocimientos                          | Descripción   |
|--|---|
| <b>Entrevistas</b>                     | A través de entrevistas al personal determinar si son conscientes y utilizan las normas establecidas por la empresa en su día a día.      |
| <b>Encuestas</b>                       | Sirven para tener un panorama general del estado de la empresa.   |
| <b>Análisis de los procesos</b>        | Las empresas deberían tener documentado sus distintos procesos para que el auditor revise que cumplan los estándares pautados.            |
| <b>Analisis del código de software</b> | Mediante distintas pruebas o análisis de la sintaxis los auditores aseguran que las pautas para el desarrollo de software sean cumplidas. |

## Seguridad Física y seguridad lógica

## Seguridad física

Consiste en el establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización —sus datos—.



### Dispositivos físicos de protección

Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.

### UPS (Uninterruptable Power Supply)

Es un dispositivo electrónico que almacena energía por medio de una batería interna. Esto le permite a los dispositivos que están conectados al mismo, frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.

## **Respaldo de datos**

Es importante saber que los datos son los activos más importantes dentro de una organización, por tal motivo, es de suma importancia el manejo y cuidado de los mismos ya que pueden estar expuestos a muchos factores como hurto, alteración, virus, entre otros. Por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales. El backup es un proceso por el cual se realiza la copia de los datos originales con el fin de prevenir cualquier tipo de pérdida de los mismos.

## **Sistemas redundantes**

Son la copia de datos de mayor importancia. Cuando uno de los sistemas falla, no se pierde la información, sino que se recupera del otro lugar donde se encuentra.

## **Seguridad lógica**

La seguridad lógica es un tipo de software que impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red. Está conformada por un conjunto de procesos que se encargan de garantizar la seguridad de los datos y sistemas, además controlan el acceso a los mismos.

Incluye aspectos como:

- Control de acceso
- Cifrado de datos
- Antivirus
- Firewalls

|                          |  |
|--------------------------|--|
| <b>Control de acceso</b> | Impide el acceso a las personas no autorizadas mediante el uso de usuarios y contraseñas.  |
| <b>Cifrado de datos</b>  | <p>El cifrado es la acción de transformar un mensaje de tal forma que no pueda ser comprendido por otra persona distinta al receptor.</p> <p>Por lo tanto, el cifrado de datos consiste en la aplicación de un algoritmo de cifrado acompañado de una clave, con el objetivo de transformar el mensaje, para que únicamente pueda ser leído por el destinatario.</p> |
| <b>Antivirus</b>         | Permite escanear, detectar y eliminar malware en un sistema informático.   |
| <b>Firewalls</b>         | Impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red.  |

## Seguridad en internet

# 1 | Ataque de denegación de servicio (DoS)

Ataques de denegación de servicios

DigitalHouse >  
Coding School

“ Cuando hablamos de la **dimensión de disponibilidad** nos referimos a que la persona debe tener acceso a la información en el momento en que la necesite, en tiempo y forma.



Ataques de denegación de servicios

DigitalHouse >  
Coding School

“

La denegación de servicio consiste en la interrupción del acceso a los servicios (computadoras y redes) por parte de los usuarios legítimos.



”

## Ataque de denegación de servicio (DoS)

En un DoS lo que sucede es que se produce una gran cantidad de peticiones desde solamente una máquina o una dirección IP al servicio, produciendo una saturación de los puertos, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones, es aquí donde se produce la denegación del servicio.

Por otro lado, un DoS no solo puede ocurrir desde la red. El incremento del uso de recursos de manera sintética o forzada (como CPU o memoria) también puede producir un DoS. Es decir, no solo puede ocurrir saturando la red, sino que también se puede saturar otros recursos y producir el mismo efecto. Y esto podría ocurrir desde la red o internamente en el servidor con algún agente instalado programado para tal fin.

**2**

## **Ataque de denegación de servicio distribuido (DDoS)**

## **Ataque de denegación de servicio distribuido (DDoS)**

En un DDoS lo que sucede es que se produce una gran cantidad de peticiones al servicio, pero en este tipo se lleva a cabo desde varios puntos o direcciones IPs de conexión produciendo la saturación del puerto de destino, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones, es aquí donde se produce el ataque de denegación de servicio distribuido.

## bot - botnes

bot: es una **aplicación de software** que se encarga de realizar las tareas que tienen la característica de ser simples y repetitivas. Las mismas se realizarán a través de Internet. Estos bots trabajan mucho más rápido de lo que trabajaría una persona.

botnet: es un conjunto de dispositivos que están conectados a Internet y que cuya seguridad ha sido comprometida por un atacante para instalar un bot programado para efectuar un ataque de DoS. Los dispositivos comprometidos quedan a la espera de que el atacante envíe una señal para comenzar el ataque.

## Computadora- Zombie

Una computadora zombie es una computadora que ha sido infectada por un virus, troyano o un gusano, y se utiliza de forma remota por un tercero, para realizar ataques maliciosos —entre ellos está el ataque de denegación de servicio distribuido DDoS—.

## 3 | Diferencia entre DoS y DDoS

Ataques de denegación de servicios

DigitalHouse >  
Coding School

“ En DoS las peticiones se realizan desde solo una máquina o una dirección IP, como también puede ser desde algún agente instalado programado para tal fin. En DDoS las peticiones se realizan desde varios puntos o direcciones IPs. ”



Ataques de denegación de servicios

DigitalHouse >  
Coding School

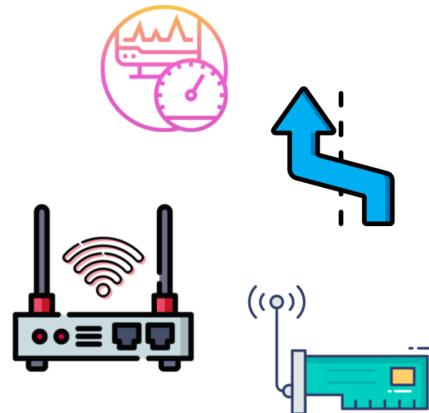
# 4 | ¿ Cómo atacan ?

## Métodos de ataque

Consumen el ancho de banda.

Alteran las tablas de enrutamiento —la ruta por donde debe ir la información—. Por tal motivo, la información que se envía no llega a destino.

Fallas en los componentes físicos de una red.



## Hacking y Cracking

Un sistema de información es un conjunto de elementos que están orientados al tratamiento y la administración de los datos para obtener información en base a ellos.

Un hacker es una persona a la cual le apasiona el conocimiento, descubrir o aprender nuevas cosas e indagar más sobre ellas. Toda aquella persona que hackea cualquier tipo de sistema descubre sus **vulnerabilidades** con el objetivo de poder encontrar alguna herramienta que la minimice o suprima —en el caso de un white hat— o utilizar esta vulnerabilidad a su favor —en el caso de un black hat— y esto lo logra en base a su conocimiento.

Y por qué no nombrar a aquellas personas que han sido hackers, por ejemplo, Rene Favaloro, un hacker en medicina, al descubrir una vulnerabilidad en el sistema cardiaco y realizar el primer bypass cardiaco.

## Tipos de hacker

- Sombrero blanco (white hats): utilizan los conocimientos en informática y seguridad informática con el fin de defender los sistemas de información.
- Sombrero gris (gray hats): tienen conocimientos tanto de la parte defensiva como ofensiva y pueden trabajar en cualquiera de los ámbitos.
- Sombrero negro (black hats): tienen conocimientos informáticos y recurren a hacer actividades maliciosas o ilegales. También conocidos como crackers.

## Las diferencias entre hacker y cracker

El **hacker** es un experto en varias ramas técnicas relacionadas con las tecnologías de información de las comunicaciones, como son: programación, redes, sistemas operativos e ingeniería de software.

El **cracker** es también un experto, pero además es quien viola la seguridad de un sistema informático con fines ilícitos o con un objetivo deshonesto y no ético.